

What is claimed is:

1 1. A method for image tamper detection, comprising the steps  
2 of:

3 (a) computing a thumbnail of an original image;

4 (b) embedding the computed thumbnail in the original image  
5 to create a marked image;

6 (c) transmitting the marked image to a recipient;

7 (d) extracting the embedded thumbnail from the transmitted  
8 marked image;

9 (e) computing a new thumbnail of the received image;

10 (f) differencing the extracted thumbnail from the new  
11 thumbnail to create a difference image that represents the  
12 similarity of the two thumbnails;

13 (g) alerting if the difference image shows the two thumbnails  
14 are not sufficiently similar; and

15 (h) authenticating the image if the difference image shows  
16 the two thumbnails are sufficiently similar.

1 2. A method for image tamper detection according to claim 1,  
2 wherein step (b) includes ensuring that the embedding does not  
3 change the size of the original image.

1 3. A method for image tamper detection according to claim 1,  
2 wherein step (b) includes ensuring that the embedding does not  
3 change the dynamic range of the original image.

1 4. A method for image tamper detection according to claim 1,  
2 wherein step (b) further comprises employing a data hiding  
3 technique that is resistant to channel noise.

1 5. A method for image tamper detection according to claim 1,  
2 wherein step (b) further comprises employing a data hiding  
3 technique that is resistant to image compression.

1 6. A method for image tamper detection according to claim 5,  
2 wherein the image compression technique is JPEG.

1 7. A method for image tamper detection according to claim 5,  
2 wherein step (b) further comprises employing a data hiding  
3 technique that is resistant to channel noise.

1 8. A method for image tamper detection according to claim 1,  
2 wherein step (b) further comprises employing a data hiding  
3 technique based on Spread Spectrum Image Stenography.

1           9.    A method for image tamper detection according to claim 1,  
2    wherein said thumbnail is defined as a low resolution version of an  
3    image.

1           10.   A method for image tamper detection according to claim 1,  
2    wherein steps (a) and (e) further comprise employing a wavelet  
3    decomposition.

1           11.   A method for image tamper detection according to claim 1,  
2    wherein step (g) further comprises thresholding the difference  
3    image to provide automatic detection of tampering.

1           12.   An apparatus for image tamper detection that creates and  
2    authenticates marked images based on thumbnail processing of that  
3    image, said apparatus comprising:

4           (a)   a memory having instructions stored therein, said  
5    instructions being executable to perform a process of thumbnail  
6    computation; and

7           (b)   a processor comprising means for executing said  
8    instructions, said instruction comprising the operations of:

9           (i)   accepting an original image or a marked image;

10 (ii) performing thumbnail processing of the accepted  
11 image  
12 to:  
13 a. derive a thumbnail of the accepted image,  
14 b. create a marked image from the accepted original  
15 image and said derived thumbnail, and  
16 c. authenticate an accepted marked image with  
17 said derived thumbnail.

1 13. The apparatus of claim 12, wherein said marked image is  
2 created by embedding said derived thumbnail in the accepted image.

1 14. The apparatus of claim 12, wherein said operation  
2 (ii)(3) includes extracting an embedded thumbnail from the  
3 accepted marked image and comparing said derived thumbnail with  
4 said embedded thumbnail for similarity.

1 15. A system for image tamper detection that creates and  
2 authenticates marked images based on thumbnail processing of that  
3 image, said system comprising:

4 (a) means for computing a thumbnail;

5 (b) means for marking an original image with said thumbnail;

6 and

7 (c) means for authenticating a marked image with said  
8 thumbnail.

1 16. A medium that stores instructions for image tamper  
2 detection that creates and authenticates marked images based on  
3 thumbnail processing of that image, adapted to be executed by at  
4 least one processor to perform the steps of:

5 (a) accepting an original or marked image;

6 (b) computing a derived thumbnail from the accepted image;

7 (c) for an accepted original image, embedding the derived  
8 thumbnail into the accepted image;

9 (d) for an accepted marked image, extracting an embedded  
10 thumbnail from the marked image; and

11 (e) for an accepted marked image, comparing said derived  
12 thumbnail with said extracted thumbnail to determine similarity.